MILITARY DECEPTION AND COUNTERDECEPTION

IW 120

OPR: Captain Winston A. Gould

DESCRIPTION: This lesson discusses the principles of military deception and counterdeception in Information Warfare.

METHODOLOGY: Informal Lecture/1.5 Hours

OBJECTIVE: The objective of this lesson plan is for each student to comprehend the principles of military deception and counter deception in Information Warfare.

SAMPLES OF BEHAVIOR:

1. Explain the relationship between military deception and U. S. Air Force doctrine.
2. Relate how military deception principles and procedures contribute to the accomplishment of Information Warfare.
3. Explain the relationship between counter deception and U. S. Air Force doctrine.
4. Relate how counter deception principles and procedures contribute to the accomplishment of Information Warfare.
5. Understand the synergistic effects of IW in relation to military deception and counter deception.

REQUIRED READINGS:

1. "Tactical Deception in Air-Land Warfare". Charles A. Fowler and Robert F. Nesbit. *Journal of Electronic Defense*. Association of Old Crows. 1995. Instruction Circular Pages 120-H-1 through 220-H-15.

Tactical Deception in Air-Land Warfare

Charles A. Fowler* and Robert F. Nesbit, Journal of Electronic Defense, June 1995

Deception in a multiplicity of forms has been a part of nearly all military operations. The literature is replete with examples throughout the history of warfare. In his 2,500-year-old classic, The Art of War, Sun Tzu states that “all warfare is based upon deception” and also notes, “Rapidity is the essence of war; take advantage of the enemy’s unreadiness, make your way by unexpected routes, and attack unguarded spots.”1 The story of the Trojan Horse is familiar to all.

Even George Washington practiced deception in the Revolutionary War by making his troop movements toward Yorktown appear to Sir Henry Clinton to be a ruse concealing a real attack on New York via Staten Island. This complex set of operations (also involving Lafayette, Cornwallis, Nathaniel Greene and the French and British navies) is described in MGen Edmund Thompson’s article “Intelligence at Yorktown.”2 From today’s perspective, the most astounding part of the story concerns General Green’s capture of some encrypted correspondence from Cornwallis to his subordinates. Greene sent the captured messages to the Continental Congress! Upon receipt, Congressman James Lovell solved the code in four days and continued to decrypt subsequent messages for the duration of the campaign. This story caused some wag to make two observations: (1) That may well have been the last useful thing Congress did, and (2) if this happened today, the next morning’s edition of the Washington Post would print the message.

HISTORICAL PERSPECTIVE

Deception operations can range in size from small unit operations, such as the MiG traps employed in the Vietnam War, to massive operations involving essentially an entire theatre, such as Operation Fortitude practiced in preparation for the Normandy invasion. Several of the more successful military deception operations in the 20th century are summarized below:

•“The Haversack Trick” was employed in the 1917 war between Great Britain and Turkey in Palestine. A British major named Meinhertzhagen deceived the Turks into thinking the British attack would be by an amphibious landing at Gaza on November 4, when the real attack was to take place at Beersheba on October 31. Major Meinhertzhagen distributed this false data by “coded” message after he had allowed the Turks to solve one of the radio codes, and then by intentionally losing his haversack that contained his lunch wrapped in official documents “confirming” the November 4 attack on Gaza. He also conducted a large effort designed to “find” the lost haversack. The Turks were caught completely off guard with their troops in the wrong place by the October 3 attack. The battleline that had been stalled for months was quickly crossed by the British and by November 9, they were in Jerusalem.4

•The German Army achieved complete strategic and tactical surprise in its 1941 invasion of Russia, largely as a result of a carefully crafted and explicitly detailed deception plan. The preparations for Operation Barbarosa were meticulously covered by surrounding them with a plethora of false rumors, poorly "encoded" misinformation, counterespionage operations and a believable cover story that Barbarosa itself was a diversion for the invasion of England. The German Army moved over 400 miles in only four weeks against the poorly prepared Russians and destroyed 1,400 Russian aircraft on the ground in just the first day.5 As Roberta Wohlstetter noted in her study of Pearl Harbor, "To understand the fact of surprise it is necessary to examine the characteristics of the noise as well as the signals that after the event are clearly seen to herald the attack."6

•"Operation Fortitude" was designed to achieve surprise in the Allied landing at Normandy in World War II. The plan was to keep the German Reserve Army at Calais by making them think that would be the location of the Allied invasion of Europe. To do this, the Allies assembled a large number of decoys across from the Pas de Calais, including decoy gliders, landing craft, tanks, trucks, guns, etc. In addition, dummy communication nets were set up to look like a command headquarters, and troops were marched in during the day, back out at night and back in the next day. "Special means" (agents) were also used to leak the deception story. Due to this deception operation, the Allies were able to land the largest invasion force in history, with the Germans thinking (for the next six weeks) that it was only a diversion.7

•One of the more famous deception schemes occurred in 1943 — "The Man Who Never Was."8 The British dressed a body as a Royal Marine Major and dropped the corpse into the sea off the coast of Spain. The corpse carried a briefcase containing documents indicating that the British planned to invade Greece. The intent of the deception was to cover the actual planned invasion of Sicily. The scheme caused the Germans to divert an entire armored division to Greece.

•The Soviets conducted a massive operation code named "Bagration" against the Germans in 1944. The offensive involved 175 Soviet divisions over a 900-km front in Belorussia. Soviet plans paid considerable attention to cover, deception, security and surprise. In order to move 50 rifle divisions from other areas of the front, they established a 25-km deep security zone from Leningrad to the Black Sea to prevent German reconnaissance. To mislead the Germans concerning the offensive in the central Belorussia region, they "demonstrated" a large-scale concentration of forces on the southern Ukrainian front and undertook an offensive on the northern Leningrad portion of the front. These efforts succeeded in masking the real region of attack and resulted in a Soviet westward advance of 550-600 km.

Some of the best examples of electronic deception are included in R.V. Jones accounts of British operations in World War II.

•German U-boats were being fixed generally by highly sensitive COMINT, and then localized by radar. But the Germans installed a radar detector called "

subs which “saw” the radar before the radar could “see” the U-boat. Thus warned, the subs could submerge and escape. Jones not only changed the frequency of the search radar so that “Metox” could not pick up the signal, but he also provided British-controlled, German agents with two bits of spurious “intelligence.” One was that the British Navy had abandoned radar for an infrared detector, and the other was that “
signal on which British aircraft could home. As a result: Not only were the Germans very slow in realizing that we were using [changed frequency] radar... but they also developed a most ingenious paint for their U-boats to camouflage them against infrared as well as against visible light....When the Germans investigated, they found there was indeed radiation coming out of the Metox receiver, and they went to some trouble to suppress it....When the Germans finally realized that we were using radar after all, they fortunately blamed it for all their U-boat sinkings..., even going so far to say that this one invention changed the balance in the Battle of the Atlantic, and our [COMINT] feat remained secure.9

•In 1941, Jones provided cover and deception for the deployment of a new radio navigation aid for RAF bombers, a synchronous pulse system known as “Gee.” He manipulated nomenclature, type numbers and equipment markings to foreshadow installation of a new piece of telegraph or voice communications gear in RAF bombers, so as to cover from German scrutiny of downed bombers or interrogation of crews the impending installation of the navigation aid. Further, Gee transmitter stations were camouflaged as radar, and irregularities were introduced into the Gee pulses to make the German electronic intelligence (ELINT) task more difficult. But these might not have worked had Jones not also authored a deception scheme to persuade the Germans that the British were about to install Lorenz beam, radio-direction-finding equipment in the bombers, for which he invented the name “Jay beams” — a real system intended for limited homing vice target designating use. Through British intelligence as well as German agents under its control, Jones provided Berlin with a report of an eavesdropped conversation between two RAF officers in which “Jay beams” were to pathfind to targets, and reports of special lectures in RAF bomber squadrons by England’s well-renowned expert on Lorenz beams. Thus led off the scent, the Germans failed to detect Gee when it was put in use (March 1942), and the British enjoyed five months of successful operations before the Germans began jamming Gee. Jones went on to say, “A final twist of the story was that when the Germans realized that they had been hoaxed they ceased to pay any attention to the Jay beams, which continued to work throughout the war, and thus provided a useful homing service for our bombers when more sophisticated aids were jammed.”9

•The Egyptians used a “conditioning” form of deception to achieve surprise in crossing the Suez Canal in 1973. Over several years they conducted repeated training exercises which the Israelis responded to at first, but eventually determined were routine. The buildup in September 1973 was designed to appear as a defensive training exercise to make the Israelis think the Egyptians feared reprisals for the Munich killings and some more recent kidnappings. Through this deception, the Egyptians gained surprise and easily crossed the canal.10

•Operation Bolo in Vietnam was very successful in luring North Vietnam MiGs into a trap. US Air Force F-4s were disguised as the less maneuverable, air-ground attack F-105s by using unique F-105 call signs and communication patterns and by carrying ECM pods previously used only on the F105. The North Vietnamese challenged the “F-105s”; in a short 12-minute air battle, the F-4s achieved complete surprise and shot down seven MiGs.11

DEFINITIONS AND SCOPE

US Joint Chiefs of Staff Publication 1 defines the intent of military deception and breaks the subject into three categories.12 “Military Deception” is defined as DOD actions executed to mislead foreign decision makers, causing them to derive and accept desired appreciation of military capabilities, intentions, operations or other activities that evoke foreign actions that contribute to the originator’s objectives. The three categories of military deception include:

a) Strategic Military Deception: Military deception planned and executed to result in foreign national policies and actions that support the originator’s national objectives, policies and strategic military plans.

b) Tactical Military Deception: Military deception planned and executed by and in support of operational commanders against the pertinent threat, to result in opposing operational actions favorable to the originator’s plans and operations.

c) Departmental/Service Military Deception: Military deception planned and executed by military services about military systems, doctrine, tactics, techniques, personnel or service operations or other activities to result in foreign actions that increase or maintain the originator’s capabilities relative to adversaries.

This paper deals only with tactical deception in air/land warfare.

A CLASSIC EXAMPLE

One particularly interesting example occurred in one of the US Army Reforger exercises. Given the terrain on which the exercise took place, it appeared most likely that the Aggressor Force would attack in the center of the front because of its geographic suitability for tank maneuver and attack. Visual signs of such activity were deceptively presented to the Defensive Force. Communications intercepted and located by the Defensive Force Guardrail system (an Army aircraft with COMINT and direction-finding capabilities) were commensurate with an attack in the central area. Finally, a scout vehicle that contained maps that fitted this mode of attack was “captured.” In other words, all of the indicators pointed to an attack in the logical, and therefore expected, central region of the front. Consequently, the Defensive Force positioned itself to inflict maximum attrition on the Aggressor Force attacking in this region.

The Aggressor Force used its Stand Off Target Acquisition System (SOTAS) to verify that the Defensive Force had indeed positioned itself in the central region; this was the necessary feedback required for any major operation. Meanwhile, under cover of night and with complete radio silence, the Aggressor Force — using trains, narrow mountain roads at night and telephone communications — came down in two salients at each side of the exercise area and had the Defensive Force cut off and essentially surrounded while the defenders were awaiting the expected frontal assault.

There are several interesting points to be made from this example.

•It shows that good commanders do include deception in their activities. They are innovative and the forces do it well.
•It points out that denial of the real activity (by use of darkness and emission control) is as important as the deception activities.
•The activity suggested by the deception was believable. In fact, it was so logical it was not challenged or subjected to skeptical scrutiny.
•The defensive force did not use its SOTAS for several reasons. Had it done so, it would have been readily apparent that the real activities were on the flanks and not in the central region.

An important point here is that a very successful, believable deception activity against the set of sensors used by the Defensive Force would not have worked against a more complete sensor set unless special provisions had been made to deceive, jam or remove the additional sensors.

As is often the case, while the exercise results indicate the tremendous benefits of deception, they also raise a number of questions. The Aggressor Force commander and his small planning staff had a number of months to work out the details of this operations plan, including the major deception activity. It is not at all clear that they would have the wherewithal to carry out this level of planning on other than an exercise basis. Nor is it clear that those who carried out the planning were aware of its vulnerability to SOTAS observation.

The conclusion to be drawn from this and other examples of tactical deception activities is that deception planning can be quite involved and complex; its execution can be quite risky, but its benefits can be overwhelming.

It should be noted for the record that the commander of the Aggressor Force who was personally involved in the innovation and guided the detailed planning of this very successful operation was MG Glen Otis, subsequently promoted to commander of TRADOC and commander, US Army, Europe at the rank of four-star general.

FUNDAMENTALS OF DECEPTION

There seem to be several fundamentals of successful tactical deception. We have dignified them here by calling them “rules.”

First Rule: To be effective, a deception operation must be one that causes the enemy to believe what he expects. To put it another way, whereas the real operation can be, in fact should be, unusual, different, even downright unbelievable (see rule number six), the deception plan must be straightforward, sensible and essentially obvious to one’s opponent.

This point is made frequently in descriptions of successful deception activities. For example, in his description of Yorktown, General Thompson notes:

about to be attacked in New York; so the ruse devised by Washington was to make the shift of the Continental Army toward Yorktown appear to be a ruse concealing a real attack on New York via Staten Island. Only too late would Clinton realize that his conceptions of ruse and reality were actually reversed.2

It has been asserted that a successful deception must contain 95% truth. This in turn suggests a corollary to this first rule. “Perhaps the bodyguard of lies would always be surrounded by a bodyguard of truth.” There is another aspect of this, of course. What a person or group expects to happen is strongly dependent on his background and culture and his view of his opponent’s background and culture. One student of deception put it this way: study and find what the opponent is a sucker for, what beliefs and biases are built into his society and culture. An important additional benefit of successful deception is that it can be a means to reduce an enemy’s confidence in his own battle performance as well as enemy troop confidence in the capacity of their commanders and fellow units.

An Israeli officer who participated in military planning, including deception activities, stressed the need to understand thoroughly the opposing force right down to the level of individual commander characteristics so that one knew what they would consider “logical.” The Israelis continue to do this for each country with which they might come into conflict.

Second Rule: Timely feedback is an essential element of all major deception operations. Feedback on the enemy’s reaction to any deception activity is critically important if one’s own position would be vulnerable should the opponent not be fooled.

Traditional means of observing reaction to deception activities have ranged from HUMINT reports by scouts or agents to intercepted communications. With current sensor

capabilities, direct observation in real- or near-real-time from stand-off distances can permit observation of an opponent's reaction to deception activities and his observation of

Third Rule: Deception must be integrated with operations. The deception plan should never be created independently from the operations plan. The practice of having a separate deception planning staff is clearly wrong. To give further emphasis to this point, there have been many cases of impromptu or "ad-libbed" deception operations that, at best, never worked and, more often than not, were counterproductive. Some Vietnam observers estimate that for every deception operation that worked there were 10 or more that didn't because they weren't tied into operations and there was incomplete knowledge of the enemy's capabilities to observe what was happening.

To put it another way, operation and deception plans must complement and supplement each other. The overall activity must not only provide believable indicators of the false operation, but must deny believable indicators of the real operations.

Fourth Rule: Denial of information on the true activities is also essential; it will depend, in significant part, on stealth and C3 countermeasures (C3CM) activities. As noted earlier, it is one thing to provide inputs to a sensor to indicate activity where none exists, and it's a different thing, in most cases, to hide the real activity.

For example, carefully constructed false radio transmissions fed to an intercept system can frequently deceive an opponent — but only if there are no contradictory emissions from the real activity. This in turn requires carrying out the real operation in a manner such that radio, radar and any other electromagnetic radiations cannot be intercepted by the opponent; a practice known as emission control (EMCON). The use of covert or low-probability-of-intercept emitters or sometimes complete radio/radar silence is required.

Other forms of stealth include use of night, cloud cover or camouflage to hide from visual observations. Some sensors are particularly difficult to deceive or deny — a Joint STARS-like stand-off moving target indicator (MTI) radar, for example. In such cases, C3CM such as jamming or attack (to destroy the sensor or drive it out of range) may be required. There is an intimate relation between tactical deception operations and stealth and C3CM activities.

It is important to note that current sensor systems, unless countered, would have permitted the detection and foiling of essentially every successful tactical deception operation ever attempted. This has major implications for both tactical deception activities and for the sensor capabilities that a country and its allies actually deploy.

Fifth Rule: The realism required for any deception activity is a function of the sensor and analysis capabilities available to the opponent and the time available to analyze the situation, disseminate the data to the appropriate points and take appropriate actions. In a low altitude attack, for example, the pilot has very little time — a matter of seconds — to

tell the difference between a decoy tank and a real tank. Thus, the quality of the decoy can be very crude and the deception will still be successful. In contrast, if one wished to indicate a build-up of tanks in a port area where there was a matter of days or longer to examine photographs of the tanks, of track prints in the earth, etc., then a high degree of realism is required.

For operations with little exposure time, minimal realism is required. Simple, cheap decoys and signal simulators can be used. There are no strict security requirements and really no need for complex feedback. One should expect that the deception will work, but should not be largely dependent upon its success.

As the need for realism increases, so does the need for feedback for assessment and for deceiving intelligence sources. This would seem to call for special organization and classification to reduce the risks of compromise and, finally, the kind of double-think, triple-think analysis that depends in substantial part on the detailed understanding of the society and culture of one's opponent.

Sixth Rule: The most effective deception will be imaginative and creative; it cannot be "legislated" or "ordered"; and it must not become stereotyped or "bureaucratized." Deception is not a subject that lends itself to strict rules, detailed regulations or regimented procedures. In fact, the worst situation would be one where "standard deception practices" were developed and institutionalized. In describing his plans for renewed emphasis on tactical deception throughout the Army, then Chief of Staff General Edward C. "Shy" Meyer noted that it would require special attention to prevent the handbook from containing something like "place one decoy tank 10 m right and 50 m below the road intersection." Military deception is best accomplished by bright, inventive (and tricky) commanders who are given the necessary tools and the latitude to use them as they see fit.

A key point to remember when reviewing the application of these rules in the modern era of improved sensors is that while the requirements for successful deception have changed, and will continue to change as the adversary acquires new sensor/intelligence capabilities, so have the opportunities. Each new sensor capability and each new communication channel to convey information and commands adds to the difficulty in carrying out unobserved operations and creating believable deception operations. On the other hand, most of these new capabilities have vulnerabilities and thus provide opportunities for deception.

The final point that stands out after looking at the overall subject of tactical deception is that commanders and their troops must be alert to and greatly concerned about being deceived by an opponent. This in turn leads to a fundamental observation: The military group that is not devoting appropriate efforts to include tactics, R&D and plotting and scheming in general for deception is almost certain to be vulnerable to being deceived itself.

This point was illustrated several times when deception practices were re-introduced in US exercises in 1983-84. In the first air exercises, simple disinformation over clear radio channels was assumed to be accurate and acted upon, leaving the deceived side very vulnerable. Two-dimensional tank decoys were completely successful the first few times they were used.

But in subsequent exercises, the deceived side was much more skeptical and regularly used cross checks for all suspicious information and situations. Any group skillful in and equipped for deception operations is less likely to be deceived. However, this knowledgeable skepticism has to be kept sharp, which presents a real problem with the frequent turnover in personnel. A prime objective of deception/counter-deception activities therefore should be a continuing effort to elevate the awareness of one's forces to the means, likelihood and impact of deception operations, both friendly and hostile.

At this point, a note about the two-dimensional tank decoys just mentioned is in order. Decoys are a particularly simple and attractive tool to be used in tactical deception operations. Their value will only increase as commercial satellite imaging systems become readily available on a worldwide basis.

Realistic decoys can be constructed in a variety of forms, including:

•Inflatable decoys, which can be assembled by a few people with a blower kit in an hour or so
•Skeletal decoys, a fairly low-fidelity approach consisting of a frame of wood or aluminum with canvas or nylon stretched over it
•Compressed foam decoys, made from a polyurethane, rather expensive, material that can be stored in a box more than 10 times smaller than its deployed size.
•Plastic decoys, a lightweight and potentially very high fidelity approach
•Multispectral decoys, with which the addition of IR and radar "signatures" can be added to most types of decoys.

SENSORS, EQUIPMENT AND SCENARIOS

We have noted that as the capability of an enemy's sensor set increases, the difficulty of deceiving these sensors also increases. Instead of "difficult" we should perhaps say the "technical challenge" of deceiving the advanced sensors increases. It is quite possible (some say probable) that, unless proper precautions are taken, overall vulnerability to deception could increase as one's sensors become more sophisticated. The converse of this is certainly true in the extreme case — an army with no sensors is impossible to deceive. The likelihood of future armies having no sensors is growing much smaller, particularly given the appearance of systems such as the French satellite imaging system SPOT and our own Landsat, whose data are normally available to anyone. Further, several other countries will deploy similar systems in the relatively near future.

With the growing array of sensors now in military inventories around the world, here are some important requirements for creating and executing good deception/denial plans:

•Knowledge of an adversary's tactics, sensors, C3 system, decision cycle time and deception approaches
•Equipment for concealment, deception and C3CM
•Planning aids and database.

Compiling a Database

It is necessary to have ready access to intelligence on enemy capabilities so one can tailor his deception and real operations to take those capabilities into account. This is becoming very complex, given the necessity for operations almost anywhere in the world. To obtain the information necessary to compile the required database, the following steps should be taken:

•Create a model of the expected observables
•Design a collection plan
•Record the visible, IR and electronic observables of the operation (e.g., a division mobilization; an air squadron deployment) on film and tape (including the radar observables)
•Analyze the tapes and compare to and revise the model
•Repeat if and as necessary
•Determine which signatures must be generated and which suppressed to make a successful deception
•Obtain equipment and create the procedures and operations required to implement the deception.

The deception database would include a handbook of "enemy" and internationally available sensors, listing the capabilities and limitations of each (e.g., the ephemeris for relevant satellites, frequency coverage and location accuracy of SIGINT aircraft; characteristics of C3 elements for getting the information to users; etc.). In addition, the database should include a good description in the appropriate form of friendly force elements and their characteristics.

Automated planning aids would allow: ready access to the database; interplay between friendly and hostile force characteristics; and the opposition's capabilities and cycle time. They also might provide a means for indicating necessary feedback quality and time criticality of the total operation.

Cover, Concealment, Camouflage and Stealth

Cover, concealment, camouflage and deception are generally subsumed under tactical deception because, as noted earlier, denial of the real activity is as important as creating the false picture.

There is a direct parallel in reducing electromagnetic radiation signatures and reducing optical/IR signatures. One might use the term “electromagnetic camouflage.” The analogy holds in covertness as well as generating a confusing environment. It is probably useful to think in terms of stealth, cover, concealment and camouflage across the board. This could include reducing electromagnetic backscatter cross sections from radar through optical frequencies and introducing confusion of the signature in the electromagnetic environment from radio through optical frequencies by means of covertness, noisy environments, difficult to distinguish patterns, etc.

During WWII, British interest and concern was so great they enlisted the services of a famous magician, Jasper Maskelyne, to help with concealment and decoy design. His many contributions are described in Reference 14.

It is a complex operation to either conceal or simulate the movement of an air squadron or an army/marine brigade. There are many signatures and there could be a large array of stand-off sensors “looking at” and “listening to” the area of interest. Before the development of stand-off sensors, the job could be accomplished by denying overflight of reconnaissance aircraft; by use of darkness and cloud cover and by EMCON combined with misleading radio communications. But this situation has changed somewhat and will change greatly with the deployment of more and better sensors — especially stand-off sensors. A new emphasis on “cover” techniques and operations is required.

Multispectral camouflage covers may introduce elements of “stealth” to combat vehicles, especially during transit on roads (that is, if the material is not suitable for use in combat due either to its fragility or being incompatible with combat operations for other reasons, such as visibility, restriction of motion, etc.). Significant reduction in radar cross section could have a major impact on target signatures performance (e.g., wheels versus tracks) and even on the basic performance of such systems as Joint STARS, ASARS and combat surveillance radars in general.

Equipment Design with Cover and Deception in Mind

deception requirements. That is, how can operations be effectively conducted without using the system during the critical deception phase, and how do you efficiently simulate its signature in the non-real force?

Fortunately, the critical need for most systems occurs during the battles, i.e., after the forces are largely deployed, and not during the lengthy deployment phase. Further, those systems which have vulnerabilities for exploitation almost always offer an opportunity for deception. A few units simulating a large operation — combined with careful EMCON of the real force — will probably continue to be an important aspect of deception operations.

Decoy aircraft and emitters simulating operations could be an important factor in increasing the survivability of forward-based VSTOL aircraft. A small number of Harrier aircraft (six or so) with a minimal amount of support equipment (communications, simple navigation aids, etc.) are sometimes forward based. Such a small deployment is well suited to employing cover and deception. Simple Harrier decoys coupled with a few signal generators could realistically simulate a false forward location; the real deployment, using camouflage and EMCON, could be hidden from many nations' sensors.

DECEPTION IN DESERT STORM

The Persian Gulf War in 1991 was replete with the effective use of cover and deception — on both sides. The Iraqi forces emphasized tactical cover, and the United States focused on operational deception.

Iraq apparently learned a valuable lesson from the 1981 Israeli raid that destroyed the Osirik nuclear reactor. Ten years later in Desert Storm, Iraq's nuclear program escaped virtually intact. Through an elaborate combination of cover, deception, mobility, hardening and dispersal, the Iraqis were able to shield their key equipment and facilities from the intense coalition air strikes.15 Their efforts in this regard continued after the war in a series of widely reported attempts to circumvent the International Atomic Energy Agency inspections. They employed sophisticated measures such as operating laboratories underneath what appeared to be bombed out buildings and crude measures such as moving key equipment into a truck which drove around a facility while the inspectors were inside.

Iraqi Scud operations were also conducted under elaborate cover schemes involving multiple hide positions, operating in darkness, use of decoys and emphasizing high mobility and short exposure times. Secretary of Defense William Perry commented recently that during the war with Iraq "we spent a lot of time and energy blowing up

Iraq also made a great effort throughout its forces to minimize RF transmissions — so much so that some have concluded the Iraqi army committed "EMCON suicide."

On the other side of the battleline, deception took a different form. Shortly after Iraq invaded Kuwait, the US intelligence community prepared a handbook of Iraqi sensors, which was essential to deception planning.

Prior to the start of the air war, the US-led coalition made a concerted effort to accustom Iraqi air surveillance operators to seeing nighttime air operations patterns similar to what would be used for the initial attack. During Desert Shield large training operations were regularly conducted (usually on Wednesday nights) involving AWACS, Rivet Joint, Tankers, ABCCC and interceptors.15 The intent was to achieve an element of surprise at the start of the air war — which began on a Wednesday night. The first night's raid was an enormous success, particularly devastating to the Iraqi air defenses.

Of course, the most elaborate and successful use of operational deception came in the cleverly crafted plan for the ground war. The famous “left hook” executed by the VII Corps devastated the Republican Guard divisions. By false radio messages, misleading troop deployments and deceptive rehearsals, Iraq had been carefully lead to expect several logical attacks: (a) an amphibious assault from the east; (b) a move north toward Baghdad through the Euphrates Valley by the XVIII Airborne Corps; and/or (c) a direct assault from Marine divisions from the south on Kuwait City.

The real main operation, the movement of a very large force 200 km to the west, was hidden from the Iraqis by “taking out their eyes” (as General Norman Schwarzkopf put it), by obtaining Russian and French cooperation (whose satellite photo systems could readily see a movement of this size) and by disciplined emission control and night operations. Aided by the speed with which the VII Corps proceeded from the west through “unnavigable desert,” coalition ground forces achieved near total surprise and a stunning victory over the Republican Guard Divisions.

Just as the Reforger commander used his SOTAS to verify that his deception plan was working, General Schwarzkopf used his Joint STARS to ascertain the Iraqis did not reposition their forces to counter the left hook. Twenty-four hours before the ground attack was launched, Joint STARS spotted one unit starting to move from its position to the west; air strikes were called in, causing the unit to move off the road into fixed positions.

It is especially noted that the “left hook” deception operation was characterized by false indications that were logical and believable; completely integrated real and deception operations; accurate and timely feedback on enemy reactions; denial of the real operation accomplished by a combination of stealth and elimination of relevant sensors and associated C3 systems; sufficient realism in the deception activity to convince the remaining Iraqis intelligence systems to keep forces largely in place until it was too late to react to the real operation; and, finally, boldness and creativity.

In short, the spectacularly successful “left hook” followed all the “rules” for an effective deception operation.

CONCLUSIONS AND RECOMMENDATIONS

Deception played a major role in achieving the rapid and overwhelming victory in the Gulf War. But a large part of the five-month Desert Shield period was required for preparation. If military leaders are to be prepared to plan such operations in a shorter period of time, we must do the following:

1.The intelligence community should provide and keep current a handbook for each threat country listing its various sensors and their capabilities to observe friendly “signatures”; a handbook describing all the relevant international sensor systems, their capabilities and

availability; and a handbook describing each threat country's deception activities and equipment, both to help the operating forces and as a calibration for the deceivers.
2.The "signatures" (physical, optical/IR and electronic) of significant air and ground operations should be measured and analyzed to provide the information needed for the creation of deception and the denial of real operations.
3.Appropriate physical decoys (e.g., tanks, aircraft, etc.) and electromagnetic simulators (communications, radars, etc.) should be procured.
4.Relevant stealth and C3CM systems and techniques necessary for denial of the real operations should be developed.
5.Means for providing feedback on enemy reactions must be established and used.
6.Deception (including the use of decoys and simulators for deception, stealth and C3CM for denial and a system for feedback) should be made an integral part of all exercises.
7.Appropriate databases and planning aids should be developed and used in these exercises to acquire the training and experience to generate meaningful ops/deception plans rapidly.
8.Appropriate training, academic and R&D programs should be established.

If we do these things, our forces should have the knowledge and preparation needed to carry out successful deception planning and execution in a timely manner, even with the worldwide growth in sensor capabilities. An additional benefit will be a heightened sensitivity of our forces to deception activities by an opponent.

REFERENCES

1.Sun-Tzu, The Art of War, 6th C. BC, various translations, including those published by Oxford University Press, Random House and Delacorte Press. 2.Thompson, Maj Gen Edmund R., Intelligence at Yorktown, Defense 81 3.Defense Science Board, Task Force on Command Support — Tactical Deception in Airland Warfare, June 1983 4.Gardner, Brian, Allenby of Arabia, Lawrence's General, Coward-McCann, New York, NY, 1966 5.Whaley, Barton, Codeword BARBAROSSA, MIT Press, Cambridge, 1973 6.Wohlstetter, Roberta, Pearl Harbor: Warning and Decision, Stanford University Press, 1962 7.Norman, Albert, Operation Overlord Design and Reality: the Allied Invasion of Western Europe, Military Service Publishing Company, Harrisburg, PA, 1952 8.Montagu, Hon. Ewen, The Man Who Never Was, Lippincott, Philadelphia, PA, 1954 9.Jones, R.V., Most Secret War, H. Hamilton, London, UK, 1978 10.Allen, Peter, The Yom Kippur War, Scribner, New York, NY, 1982 11.Momyer, William W., Airpower in Three Wars, US Government Printing Office, 1983 12.Joint Chiefs of Staff, JCS Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, US Government Printing Office, 1994 13.Daniel, Donald C. and Katherine L. Herbig, editors, Strategic Military Deception, Pergamon Press, New York, NY, 1982 14.Fisher, David, The War Magician, Cowan-McCann, 1983. 15.Cohen, Eliot A., director, Gulf War Air Power Survey, US Government Printing Office, 1993 16.Jane's Defence Weekly, February 18, 1995

Charles A. Fowler is president of C.A. Fowler Associates, a member and past president of the Defense Science Board and a past member of the JED Advisory Board.

Robert F. Nesbit is vice president of the Center for Integrated Intelligence Systems at the Mitre Corp.
---

*Authors' Note: This paper derives in significant part from a 1982-83 Defense Science Board (DSB) study for the chairman of the Joint Chiefs of Staff, Gen David Jones.3 Norman Augustine, the chairman of the DSB, considered the findings and recommendations to be of such significance that he wrote in his memoir forwarding the report to the secretary of defense, "It is my belief that this may be the most important report I submitted to you during my three-year chairmanship of the board." The succeeding chairman, Gen John Vessey, directed that the study be widely briefed and distributed throughout the services and commands. As a result, it had a major impact on US actions in this area.

The authors were participants in that DSB effort and have followed this field with interest since. Besides the authors of this article, participants in the study included Dr. Davis B. Bobrow, the late GEN William E. DePuy, USA (ret.), Gen Robert J. Dixon, USAF (ret.), Dr. Eugene G. Fubini, Dr. Robert Hermann, ADM Isaac C. Kidd, Jr., USN (ret.), Dr. Joshua Lederberg, LG Phillip D. Shutler, USMC (ret.) and the late Dr. Clarence H. Stewart. CAPT Joseph A. Muka, Jr., USN, served as executive secretary; COL Wayne B. Davis, USA, was the DSB Secretariat point of contact; Walter Jajko was the DUSDP point of contact; and John M. Porter was the USDRE point of contact. We would like to acknowledge the contributions of these other members; of DSB Chairman Augustine, who helped initiate the effort and also made a number of valuable suggestions; of of Gen Paul Gorman, who as a special assistant to the CJCS was an active participant in the early days of the effort and made several useful inputs.

While fully acknowledging these contributions, we assume total responsibility for the extraction, update and expansion of the DSB work. We further note that this paper represents our views and does not purport to represent those of the DOD, the DSB or any other person or organization.